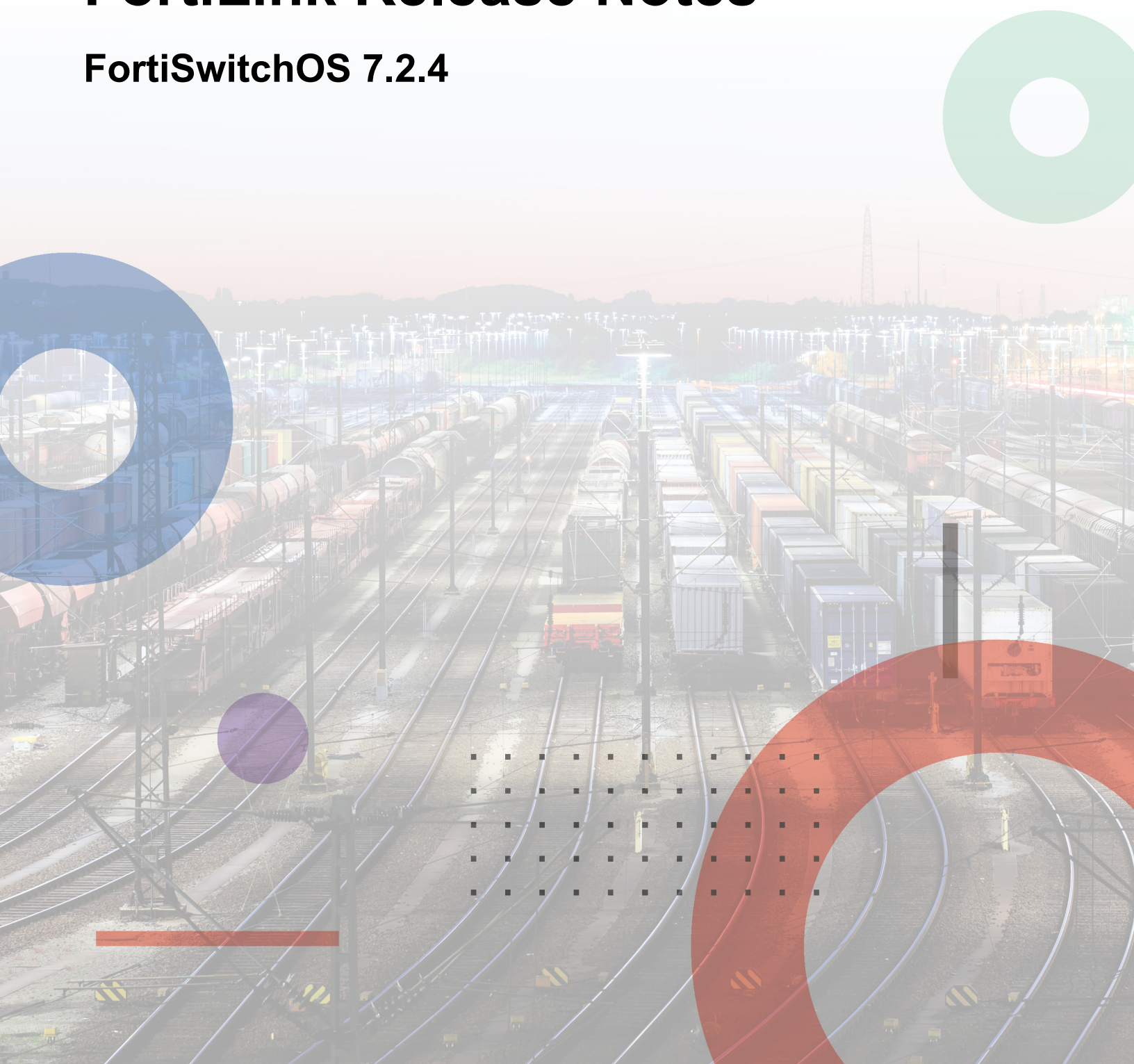
FortiLink Release Notes

FortiSwitchOS 7.2.4



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 7, 2023
FortiSwitchOS 7.2.4 FortiLink Release Notes
11-724-857161-20230307

TABLE OF CONTENTS

Change log

Date	Change Description
January 31, 2023	Initial document release for FortiOS 7.2.4
March 7, 2023	Updated the “Introduction” section.

Introduction

This document provides the following information for FortiSwitch 7.2.3 devices managed by FortiOS 7.2.4 build 1396:

See the Fortinet Document Library for FortiSwitchOS documentation.

Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

NOTE: FortiLink is not supported in transparent mode.

The maximum number of supported FortiSwitch units depends on the FortiGate model:

FortiGate Model Range	Number of FortiSwitch Units Supported
FortiGate 40F, FortiGate-VM01	8
FortiGate 6xE, 8xE, 90E, 91E	16
FGR-60F, FG-60F, FGR-60F-3G4G, FG-61F, FG-80F, FG-80FB, FG-80FP, FG-81F, and FG-81FP	24
FortiGate 100D, FortiGate-VM02	24
FortiGate 100E, 100EF, 100F, 101E, 140E, 140E-POE	32
FortiGate 200E, 201E	64
FortiGate 300D to 500D	48
FortiGate 300E to 500E	72
FortiGate 600D to 900D and FortiGate-VM04	64
FortiGate 600E to 900E	96
FortiGate 1000D to 15xxD	128
FortiGate 1100E to 26xxF	196
FortiGate-3xxx and up and FortiGate-VM08 and up	300

New models (NPI releases) might not support FortiLink. Contact Customer Service & Support to check support for FortiLink.

What's new in FortiOS 7.2.4

The following list contains new managed FortiSwitch features added in FortiOS 7.2.4:

- A new CLI command reports device statistics when network access control (NAC) is enabled. The `diagnose switch-controller telemetry show mac-stats` command reports the MAC addresses of known devices, the number of packets and bytes received, the number of seconds since the last update, and the age of the MAC counter in seconds.
- NAC now supports more connected devices—up to 48 times the maximum number of managed FortiSwitch units supported on the FortiGate device. You can use the `diagnose switch-controller mac-device nac known` command to check the number of known devices. When 95 percent of the maximum number of devices is reached, a warning icon is displayed in the *Matched NAC Devices* widget in the FortiOS GUI. When the maximum number is reached, a switch-controller event is logged.
- The range and default values for the `set nac-periodic-interval` command (under `config switch-controller system`) have changed. The default value is now 60, and the range of values is now 5-180.
- The range and default values for the `set dynamic-periodic-interval` command (under `config switch-controller system`) have changed. The default value is now 60, and the range of values is now 5-180.
- You can now specify static entries for DHCP snooping and dynamic ARP inspection (DAI) by manually associating an IP address with a MAC address in the FortiOS CLI.
- The FG-180xF and FG-260xF models can now manage 196 FortiSwitch units.
- There is now a `set link-status` command under `config switch-controller managed-switch` in the FortiOS CLI.
- New tests have been added to the FortiSwitch recommendations in the *Security Fabric* > *Security Rating* page to help optimize your network. The tests check the following:
  - If the `poe-status` has been enabled under the `config switch-controller auto-config policy` command, FortiOS recommends that you disable it to prevent unpredictable problems caused by connecting two power sourcing equipment (PSE) ports.
  - If port 8 of an FS-108E or FS-108 unit is used for an inter-switch link (ISL), FortiOS recommends creating a custom auto-config policy.
  - If the configured speed is less than the maximum speed for a switch port, FortiOS recommends changing the port speed to the maximum amount.
  - Check if the inter-switch links (ISLs) and inter-chassis links (ICLs) are static to increase stability during events such as cable disconnections or power outages.
  - When a multichassis LAG (MCLAG) is recommended between two FortiSwitch units, there is a *Create MCLAG button* available under *WiFi & Switch Controller* > *Managed FortiSwitches* in the *Topology* view.
- A new *FortiView Internal Hubs* monitor in FortiOS will report the IP addresses and the number of bytes collected with flow tracking from devices behind a managed FortiSwitch unit. If you drill down on one of the devices, you can see a chart displaying the devices and how they are connected.
- You can now use the FortiOS CLI to configure the Power over Ethernet (PoE) port mode (IEEE802.3 AF or IEEE802.3 AT), port priority (critical, high, medium, or low), and port power (normal, perpetual, or perpetual fast) on managed switches.

Special notices

Support of FortiLink features

Refer to the FortiSwitchOS feature matrix for details about the FortiLink features supported by each FortiSwitchOS model.

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.

If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

If you do not want to convert the format of the FortiSwitch admin password, you can use the FortiOS CLI to override the managed FortiSwitch admin password with the FortiGate admin password.

To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following FortiSwitchOS CLI command to convert the admin password from SHA256 to SHA1 encryption:

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

To override the managed FortiSwitch admin password with the FortiGate admin password:

```
config switch-controller switch profile
   edit <FortiSwitch_profile_name>
      set login-passwd-override enable
      set login-passwd <new_password>
   end
```

NAC policies not maintained or converted when upgrading from 6.4 to 7.2

When you upgrade from FortiOS 6.4 to FortiOS 7.2.0, existing NAC policies are not maintained or automatically converted into dynamic port policies. They have to be reconfigured.

Upgrade information

FortiSwitchOS 7.2.3 supports upgrading from FortiSwitchOS 3.5.0 and later.

To determine a compatible FortiOS version, check the FortiLink Compatibility matrix.

Within the Security Fabric, the FortiSwitch upgrade is done after the FortiGate upgrade. Refer to the latest *FortiOS Release Notes* for the complete Security Fabric upgrade order.

Product integration and support

FortiSwitchOS 7.2.3 support

The following table lists FortiSwitchOS 7.2.3 product integration and support information.

Web browser	• Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

Resolved issues

The following issues have been fixed in FortiOS 7.2.4. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
719476	The FortiLink NAC matched device is displayed in the CLI but not in *WiFi & Switch Controller* > *NAC Policies* > *View Matched Devices*.
825377	When the VDOM is enabled, some pages in the GUI are slow to display or do not display.
825505	Devices are lost in the *Users & Devices* widget after a period of time (around two days) in configurations with FortiSwitch units, FortiAP units, and DHCP.
828901	FortiSwitch and FortiAP units are disconnected when the wireless system daemon (hostapd) crashes.
831439	Multiple DHCP servers can be configured for the same range on an interface when the interface name contains a comma.
836604	The command for the managed switch port speed for a 40-Gbps copper interface was missing. You can now select `set speed 40000cr4`.
840310	A managed FortiSwitch unit only shows one port of the FortiLink aggregate interface.
858113	When the admin profile was created on a FortiGate device, the *Diagnostics and Tools* page for a FortiSwitch unit cannot be displayed with limited access permissions.

Known issues

The following known issues have been identified with FortiOS 7.2.4. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
298348, 298994	Enabling the `hw-switch-ether-filter` command on the FG-92D model (the default setting) causes FortiSwitch devices to not be discovered.
520954	When a “FortiLink mode over a layer-3 network” topology has been configured, the FortiGate GUI does not always display the complete network.
527695	Starting in FortiOS 6.4.0, VLAN optimization is enabled by default (`set vlan-optimization enable` under `config switch-controller global`). On a network running FortiSwitchOS earlier than 6.0.0, this change results in a synchronization error, but the network still functions normally. If you have FortiSwitchOS 6.0.x, you can upgrade to remove the synchronization error or disable VLAN optimization. On a network with `set allowed-vlans-all enable` configured (under `config switch-controller vlan-policy`), the setting reverts to the default, which is disabled, when upgrading to FortiOS 6.4.0. If you want to maintain the allowed-vlans-all behavior, you can restore it after the upgrade.
586801	NetBIOS stops working when proxy ARP is configured and the access VLAN is enabled because FortiGate units do not support NetBIOS proxy.
621785	`user.nac-policy[].switch-scope` might contain a data reference to `switch-controller.managed-switch`. When this reference is set by an admin, the admin needs to remove this reference before deleting the `managed-switch`.
789914	• When LAN segments are enabled on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models, the internal VLAN (`set lan-internal-vlan`) is assigned automatically by default. If the same VLAN is configured on the FortiGate device, the configuration fails when it is pushed to the FortiSwitch unit without any warning message. **WORKAROUND:** Use a custom command. • All sub-VLANs must belong to the same MSTP instance if the FortiLink configuration includes the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models.
813216	After CAPWAP offload is enabled or disabled, FortiLink goes down.
814674	When upgrading a FortiAP or FortiSwitch unit that is connected to a downstream FortiGate device, a “Failed to retrieve upgrade progress” message appears.

www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.